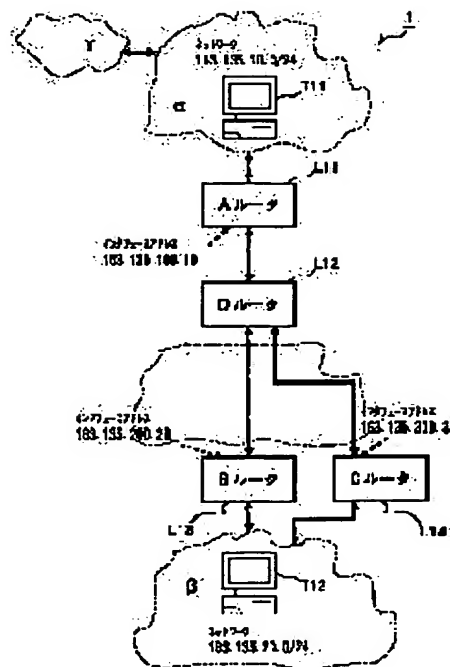


(11)Publication number : 2000-341324
(43)Date of publication of application : 08.12.2000

H04L 29/14

(72)Inventor : KUSAKA TAKAYOSHI
MATSUDA YOSHIYUKI
BABA TATSUYA

SOLUTION: Layout information relating to the layout of other routers L12 to L14 capable of cipher communication is included in path forming information of a router L11 that receives or transmits the path information such as a routing protocol. In the case that any router such as the router L13 on an optimum path during the cipher communication is disabled or communication, a new optimum path is formed again and continues the cipher communication with the other router L14 in existence on the optimum path formed again by using a key decided mutually.



09.12.2004

Best Available Copy

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2000-341324
(P2000-341324A)

(43)公開日 平成12年12月8日(2000.12.8)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)	
H 0 4 L	12/56	H 0 4 L 11/20	1 0 2 D	5 J 1 0 4
	9/08		6 0 1 Z	5 K 0 3 0
	12/46		3 1 0 C	5 K 0 3 3
	12/28			5 K 0 3 5
	12/22		3 1 1	9 A 0 0 1

審査請求 未請求 請求項の数10 O L (全 9 頁) 最終頁に続く

(21)出願番号 特願平11-146948
(22)出願日 平成11年5月26日(1999.5.26)

(71)出願人 000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号
(72)発明者 日下 貴義
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内
(72)発明者 松田 栄之
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内
(74)代理人 100099324
弁理士 鈴木 正剛

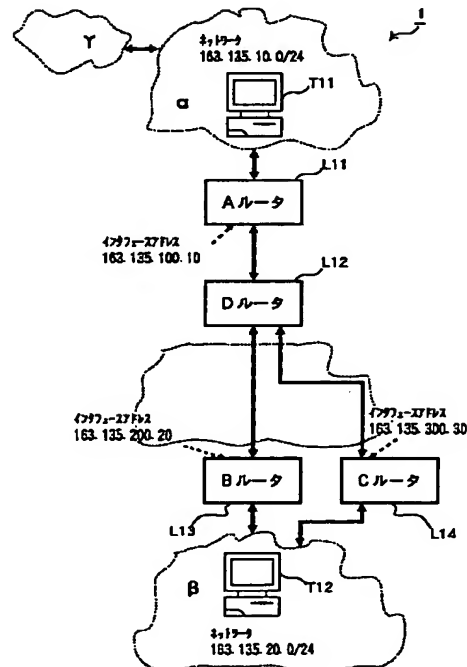
最終頁に続く

(54)【発明の名称】 暗号通信方法及びシステム

(57)【要約】

【課題】 暗号通信中に経路障害が発生し、経路変更に伴って復号化を行う装置が変わった場合にも暗号通信を継続できる暗号通信システムを実現する。

【解決手段】 ルーティングプロトコルのような経路形成情報の受け渡しを行うルータL11の経路形成情報に、暗号通信可能な他のルータL12～L14の配置に関する配置情報を含める。暗号通信中の最適経路上のいずれかのルータ、例えばルータL13が通信不能になったときは、新たな最適経路を再形成するとともに、再形成された最適経路に存する他のルータL14との間で相互に決めつけた鍵を用いて暗号通信を継続する。



【特許請求の範囲】

【請求項1】 高可用通信と暗号通信とを同時に実現することができるネットワークを介して行う暗号通信方法であって、

前記ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことによりネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行うとともに、前記ネットワーク上における通信中継装置の構成が変更された場合に前記経路形成情報を更新して新たな最適経路を再形成し、再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続することを特徴とする、暗号通信方法。

【請求項2】 各通信中継装置は、ある通信装置又はネットワークへ向かう暗号化された通信データの復号化ができる場合にその通信装置又はネットワークの識別情報を記録しておき、他の通信中継装置から前記経路形成情報を受け取ったときに暗号通信先が前記識別情報と同じ識別情報を保持していた場合に、前記他の通信中継装置との間で前記鍵の取り決めを行うことを特徴とする、請求項1記載の暗号通信方法。

【請求項3】 所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことにより高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行う暗号通信システムであって、

各通信中継装置の経路形成情報は、前記ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、

前記複数の通信中継装置の少なくとも一つは、暗号通信中の最適経路上の通信中継装置の配置構成が変更になったことを検知したときに当該変更後の配置情報を他の通信中継装置に通知するように構成され、少なくとも他の一つは、前記通知をもとに自己の経路形成情報を更新して新たな最適経路を再形成するとともに再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続するように構成されていることを特徴とする、

暗号通信システム。

【請求項4】 所定の経路形成情報をもとに高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成するとともにこの最適経路に存在する他の通信中継装置との間で暗号通信を行う通信中継装置であって、

前記経路形成情報は、暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、

暗号通信中に前記最適経路における他の通信中継装置の

配置構成が変更になった場合に自己の経路形成情報に含まれる前記配置情報の内容を更新する更新手段と、更新後の経路形成情報をもとに新たな最適経路を形成する経路形成手段と、

新たに形成された最適経路上の暗号通信可能な他の通信中継装置を検出する検出手段とを備え、

当該検出した通信中継装置との間で取り決めた鍵を用いて暗号通信を継続することを特徴とする、

通信中継装置。

10 【請求項5】 前記経路形成情報が所定のルーティングプロトコルに基づいて他の通信中継装置との間で相互に受け渡しされる情報であって、暗号通信を行えるノードの配置に関する情報及びそのノードが暗号通信実施の対象とする通信経路の識別情報を含むものであり、前記識別情報に基づいて前記鍵を取り決めることを特徴とする、

請求項4記載の通信中継装置。

20 【請求項6】 前記識別情報をもつノードとの間で取り決めた鍵を予め保持している場合はその鍵を索出し、鍵を保持していない場合は当該ノードとの間で鍵生成を行うことで前記鍵を確保することを特徴とする、

請求項5記載の通信中継装置。

【請求項7】 前記更新手段は、暗号通信中に通信不能となった通信中継装置に関する配置情報を削除するように更新することを特徴とする、

請求項4記載の通信中継装置。

【請求項8】 前記更新手段は、暗号通信中に増設された通信中継装置に関する配置情報を追加するように更新することを特徴とする、

30 請求項4記載の通信中継装置。

【請求項9】 前記更新手段は、暗号通信中に移動された通信中継装置に関する配置情報を修正するように更新することを特徴とする、

請求項4記載の通信中継装置。

【請求項10】 暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報をもとに、高可用通信と暗号通信とを同時に実現することができるネットワークネットワーク上における最適経路を形成する機能と、

40 通信相手装置との間で暗号通信を行う機能と、

前記通信相手装置の構成が変更になった場合に自己の経路形成情報に含まれる前記配置情報の内容を更新し、更新後の経路形成情報をもとに新たな最適経路を形成するとともに、この新たな最適経路に存在する他の通信相手装置との間で取り決めた鍵を用いて暗号通信を継続する機能とをコンピュータ上に形成するためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体。

【発明の詳細な説明】

50 【0001】

【発明の属する技術分野】本発明は、高可用通信（障害時でも経路切替による自動継続が可能な通信、つまり耐障害性をもつ通信、以下同じ）と暗号通信（暗号技術を利用した機密通信、以下同じ）とが同時に実現できるネットワークにおいて、暗号通信中に通信中継装置の構成の変更が生じ、最適経路が変化した場合であっても暗号通信を安全に継続できるようにするための暗号通信技術に関する。

【0002】

【従来の技術】IP（Internet Protocol）ネットワークを使用して行う暗号通信の形態は、従来より良く知られている。この種の暗号通信は、送信側の暗号化装置と受信側の復号化装置との間で生成した鍵（暗号鍵／復号鍵）を用いて行われる。この場合の通信の形態としては、エンド・ツー・エンドで暗号通信を行う形態と、通信経路上に通信データ、例えばパケットの暗号化及び復号化を行う通信装置（以下、「暗号装置」）を配置することによって暗号通信を行う形態とがある。

【0003】IPネットワークにおいて暗号通信に用いる鍵の生成、鍵交換、鍵設定の手順としては、例えばIKE（Internet Key Exchange：暗号鍵生成手順）方式等、様々な手法が存在する。送信側は、この生成された鍵（暗号鍵）を使用してIPパケットを暗号化し、受信側は、この鍵に対応した鍵（復号鍵）を用いてパケットを復号化する。

【0004】ところで、IPネットワークを使用して通信を行っている最中に最適経路に何らかの障害が発生した場合は、OSPF（Open Shortest Path First）等のルーティングプロトコルを使用したり、ルータ等の通信中継装置自身の持つバックアップ経路設定機能を使用したりして通信を回復させることができる。つまり、自動的に迂回経路を設定して通信を回復させることができる。以下、これらの通信回復方法の概要を説明する。

【0005】（1）ルーティングプロトコルを使用した場合

図6に示すように、通信装置T11と通信装置12との間のIPネットワーク上のノードにルータN11～N15が接続されているとする。正常時の最適経路は、通信装置T11→ルータN11→ルータN12→ルータN13→ルータN15→通信装置T12、あるいはその逆であり、各ルータN11～N15は、互いに持っている経路形成情報、すなわち各ルータが直接どのルータと通信可能か等を表す情報を交換し合い、ネットワーク間の最適経路を形成している。

【0006】この最適経路において、ルータN13に障害が発生した場合は、以下のような手順で通信の回復を行う。まず、ルータN13に隣接する正常なルータ、例えばルータN12が、ルーティングプロトコルの機能により、ルータN13に障害が発生したことを検知する。検知方法は、ルーティングプロトコルによって決められ

ている。障害を検知したルータN12は、「今までの経路が使用できなかったこと」や「リンクが無くなったこと」等の情報を、ルーティングプロトコルの機能により、隣接するルータN11、N14に通知する。これらの通知情報は、隣接するルータN15にもリレーされ、これによりルーティングドメイン（ルーティング情報を受け渡すルータのグループ）のすべてのルータに通知される。このように新しく通知される情報により、各ルータN11、N12、N14、N15が持つ経路形成情報は更新され、障害経路の代わりになる迂回経路、すなわち、通信装置T11→ルータN11→ルータN12→ルータN14→ルータN15→通信装置T12の経路が再形成される。

【0007】（2）バックアップ経路設定機能を使用した場合

図6に示した通信システムの中のあるルータ、例えばルータN12にバックアップ経路設定機能があり、ルータN12が中継経路に障害が発生したことを検知した場合（リンクの有無やポーリング（監視信号）、キープアラーム（回線がダウンしていないことを確かめるための信号）等による）、ルータN12は、バックアップ経路設定機能に基づいて、予め設定しておいた代替経路（バックアップ経路）に切り替えて通信を保つ。

【0008】

【発明が解決しようとしている課題】通常通信のみならず、暗号通信を行っている最中に最適経路に障害が発生した場合も、上記のルーティングプロトコルの機能やバックアップ経路設定機能を用いて迂回経路を形成することができる。しかしながら、暗号通信の場合は、ルーティングプロトコルの機能あるいはバックアップ経路への切替機能と暗号通信の機能とが別構成になっているため、既存の仕組みのままでは、暗号化されたIPパケット（暗号化データ）を復号化することができず、暗号通信を継続できない場合がある。このことを以下に説明する。

【0009】ここでは、図7に示す構成、すなわち、ルータN12に暗号装置M21を介して通信装置T11が接続され、ルータN15に通信装置T22が接続され、さらにルータN12とルータN15との間に、それぞれ暗号装置M22、M23が並列に接続されたIPネットワーク構成を想定する。

【0010】各ルータN12、N15及び暗号装置M21、M22は、互いに持っている経路形成情報を交換しあい、ネットワーク間の最適経路を形成している。正常時における最適経路、つまり通常経路で収束した場合の経路は、通信装置T11→暗号装置M21→ルータN12→暗号装置M22→ルータN15→通信装置T12であり、暗号装置M21は、通信装置T22から送信されるパケットを、自装置と暗号装置M22との間で用いられる鍵（例えば鍵A）を用いて暗号化する。

10

20

30

40

50

【0011】この状態で、暗号装置M22で何らかの障害が発生し、ルーティングプロトコルの機能により経路変更が行われ、最適経路が通信装置T11→暗号装置M21→ルータN12→暗号装置M23→ルータN15→通信装置T12に自動的に変更されたとする。この場合、暗号装置M21と暗号装置M23との間で用いられる鍵（例えば鍵B）は、前述した鍵Aとは異なっている。しかし、暗号装置M21では、パケットの送信先（通信装置T12）に変更がないので、通信装置T11から通信装置T12宛に送信されるデータの暗号用鍵を鍵Aから鍵Bに変更すべきであることを従来のルーティングプロトコルからは認識することができない。そのため、当該パケットは暗号装置M21で鍵Aで暗号化されることになり、鍵Bを用いる暗号装置M23ではこれを復号することができないので、結局、暗号通信を回復することができない。

【0012】暗号通信には、送信先のアドレスを含むIPヘッダとパケットのデータ部分（すなわちペイロード）をまとめて暗号化し、新たな送信先（復号化装置）のアドレスを含むIPヘッダを付して通信を行うトンネルモードと、送信先アドレスは暗号化せず、パケットのデータ部分だけを暗号化するトランスポートモードとがあるが、いずれのモードでも、上記のように暗号装置M22で障害が発生したときに、暗号装置M21では鍵の変更の必要性を認識することができない。

【0013】このような問題は、暗号通信中に経路障害が発生した場合のみならず、それまで最適経路であった箇所（ノード）に、新たにルータ、暗号装置、通信装置等が増設された場合や、ルータ等の一部が移動した場合においても共通に生じる。これは、従来のこの種の高可用通信におけるルータ等の配置が固定的であり、暗号通信に用いられる鍵も固定的であったことに起因する。

【0014】そこで本発明は、高可用通信と暗号通信とが同時に実現できるネットワークにおいて、暗号化及び復号化を行う装置の配置構成に変更が生じた場合であっても、暗号用の鍵を動的に変更して暗号通信を安全に継続できるようにする技術を提供することを主たる課題とする。

【0015】

【課題を解決するための手段】上記課題を解決ため、本発明は、改良された暗号通信方法、暗号通信システム、通信中継装置、及び通信中継装置をコンピュータにより実現する上で好適となる記録媒体を提供する。

【0016】本発明の暗号通信方法は、高可用通信と暗号通信とを同時に実現することができるネットワークを介して行う方法であって、ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことによりネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信デ

タの暗号通信を行うとともに、前記ネットワーク上における通信中継装置の構成が変更された場合に前記経路形成情報を更新して新たな最適経路を再形成し、再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続することを特徴とする。各通信中継装置は、ある通信装置又はネットワークへ向かう暗号化された通信データの復号化ができる場合にその通信装置又はネットワークの識別情報を記録しておき、他の通信中継装置から経路形成情報を受け取ったときに暗号通信先が前記識別情報と同じ識別情報を保持していた場合に、前記他の通信中継装置との間で鍵の取り決めを行うようにする。

【0017】本発明の暗号通信システムは、所定の経路形成情報を複数の通信中継装置間で互いに交換しあうことにより高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成し、この最適経路に存在する通信中継装置間で通信データの暗号通信を行う暗号通信システムである。各通信中継装置の経路形成情報は、前記ネットワーク上で暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、複数の通信中継装置の少なくとも一つは、暗号通信中の最適経路上の通信中継装置の配置構成が変更になったことを検知したときに当該変更後の配置情報を他の通信中継装置に通知するように構成され、少なくとも他の一つは、前記通知をもとに自己の経路形成情報を更新して新たな最適経路を再形成するとともに再形成された最適経路に存する暗号通信可能な通信中継装置間で相互に取り決めた鍵を用いて前記暗号通信を継続するように構成されていることを特徴とする。

【0018】本発明の通信中継装置は、所定の経路形成情報をもとにネットワーク上における通信データの最適経路を形成するとともにこの最適経路に存在する他の通信中継装置との間で暗号通信を行う通信中継装置において、前記経路形成情報は、暗号通信可能な通信中継装置の配置に関する配置情報を含むものであり、暗号通信中に通信相手となる他の通信中継装置が通信不能になったときに自己の経路形成情報に含まれる前記配置情報の内容を更新する手段と、更新後の経路形成情報をもとに新たな最適経路を形成する手段と、新たに形成された最適経路上の暗号通信可能な他の通信中継装置を検出する手段とを備え、当該検出した通信中継装置との間で取り決めた鍵を用いて暗号通信を継続することを特徴とする装置である。

【0019】経路形成情報は、より具体的には所定のルーティングプロトコルに基づいて他の通信中継装置との間で相互に受け渡しされる情報であって、暗号通信を行えるノードの配置に関する情報及びそのノードが暗号通信実施の対象とする通信経路の識別情報を含むものであり、この識別情報に基づいて前記鍵を取り決めるようにする。識別情報をもつノードとの間で取り決めた鍵を予

め保持している場合はその鍵を索出し、鍵を保持していない場合は当該ノードとの間で鍵生成を行うことで前記鍵を確保するようにする。

【0020】通信中継装置における更新手段は、暗号通信中に通信不能となった通信中継装置がある場合はそれに関する配置情報を削除し、暗号通信中に増設された通信中継装置がある場合はそれに関する配置情報を追加し、暗号通信中に移動された通信中継装置がある場合はそれに関する配置情報を修正する。

【0021】本発明が提供する記録媒体は、暗号通信可能な通信中継装置の配置に関する配置情報を含む所定の経路形成情報をもとに、高可用通信と暗号通信とを同時に実現することができるネットワーク上における最適経路を形成する機能と、通信相手装置との間で暗号通信を行う機能と、前記通信相手装置の構成が変更になった場合に自己の経路形成情報に含まれる前記配置情報の内容を更新し、更新後の経路形成情報をもとに新たな最適経路を形成するとともに、この新たな最適経路に存在する他の通信相手装置との間で取り決めた鍵を用いて暗号通信を継続する機能とをコンピュータ上に形成するためのプログラムコードが記録された、コンピュータ読みとり可能な記録媒体である。

【0022】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。本発明では、高可用通信と暗号通信とが同時に実現できるネットワークにおいて、ルーティングプロトコルに従って経路形成情報の受け渡しを行う装置間で暗号通信を行っている場合に、暗号通信が可能な装置の配置に関する情報を上記経路形成情報に含め、経路形成情報と鍵の変更に関する情報とをリンクさせるようにする。例えば、リンクステート式のルーティングプロトコルであれば、どのリンクに暗号通信可能な装置が配置されていてどのネットワーク間で暗号通信を行えるのか、ディスタンスベクトル式のルーティングプロトコルであれば、その距離ベクトル中にどのルータが存在するかを、経路形成情報の中に含める。そして、暗号化データを送信する際に、受信先の暗号装置に対応した鍵を用い、対応した鍵が無ければ新たに生成する、ということを経易に行えるようにする。なお、鍵の使用・生成は、従来から一般的に用いられていた手法を利用することができる。

【0023】上述の暗号通信方法は、例えば図1に示すように構成される暗号通信システムによって実施することができる。この暗号通信システム1は、 α ネットワーク上に配された送信側の通信装置T11、 β ネットワーク上に配された受信側の通信装置T12、これらの通信装置間に介在する複数のルータ、すなわちAルータL11、DルータL12、BルータL13、CルータL14その他のネットワーク構成部品を含み、高可用通信と暗号通信とを同時に実現できるように構成される。 α ネッ

トワークと β ネットワークとはインターネットのような広域通信網を介して接続されているものとする。

【0024】各ルータL11～L14は、メモリ及びCPUを有する一種のコンピュータであり、そのCPUが所定の記録媒体に記録されたプログラムコードを読み込んで実行されることによって形成されるルーティングプロトコルの機能、暗号通信の機能、及び、これらの機能を連携させる機能を有する。このプログラムコードを記録した記録媒体は、ルータに実装されるときには、例えばCPUが読みとり可能な半導体メモリ等の固定型記録媒体であるが、CD-ROM等の可搬性記録媒体を通じて流通し、実装時に上記固定型記録媒体にインストールされるものであっても良い。ルーティングプロトコルの機能については、従来のルータのものと基本的には同じであるが、ルーティングプロトコルで他のルータと交換する経路形成情報に次の二つの情報を含め、暗号通信の機能を連携させるようにした点で従来のルータが備える機能と異なる。

(1) 暗号通信を行えるノード(ルータ)の配置やインタフェースID

例:「暗号通信ができるAノードにAルータがある」

(2) そのノードが暗号通信実施の対象とする通信経路ID

例:「Aルータにおける暗号通信の対象(通信経路ID)は、 α ネットワーク及び β ネットワークの通信に対するものである」

これらの情報に対応するデータの形式は、適応するネットワークプロトコルやルーティングプロトコルに合わせたものになる。例えばIPネットワークのOSPFの場合は、後述するLSA(Link State Advertisement)にその情報を含めることになる。

【0025】一方、暗号通信の機能に関して、各ルータは、以下のようにして暗号通信を行う。

(1) 暗号通信実施対象の通信経路IDに対応する通信に対して、通信データ、例えばパケットを暗号化し、暗号化データを生成する。

例:「Aルータを通過するパケットのソースアドレスが β ネットワークに属し、ディスティネーションアドレスが β ネットワークに属するパケットは、ディスティネーションアドレスが通信経路IDに適合するので、暗号通信の対象とする」

(2) 暗号用の鍵は、通信経路に対応する通信経路IDを持ったノードのものを予め保持している場合はそれを索出して使用する。鍵を保持していない場合は、そのノード(ルータ)との間で鍵生成を行うことで、鍵を確保する。

例:「Aルータから β ネットワーク宛の経路上に、Bルータという暗号通信が可能なルータが存在し、そのBルータが β ネットワークに対して暗号通信実施の対象としていることを、ルーティングプロトコルによりAルータ

は知っている。そこで、暗号通信の対象となったパケットをBルータに対応する鍵を使用して暗号化する」両者の機能をリンクさせる機能については後述する。

【0026】なお、以上の機能は、全てのルータL11～L14が備えていることが望ましいが、通信装置T11から送られたパケットを暗号化して中継するいずれか中心的に作用するルータのみが備えている場合であっても本発明の実施は可能である。

【0027】次に、本実施形態の暗号通信システム1による通信形態を説明する。ここでは、図示のように、αネットワーク内の通信装置T11とAルータL11間のネットワークアドレスが「163.135.10.0/24」、βネットワーク内の通信装置T12とBルータL13又はCルータL14との間のインタフェースアドレスが「163.135.20.0/24」、AルータL11のインタフェースアドレスが「163.135.100.10」、BルータL13のインタフェースアドレスが「163.135.200.20」、CルータL14のネットワークアドレスが「163.135.300.30」であるものとし、リンクステート式ルーティングプロトコルの代表である上記OSPFの改良を行って暗号通信を行う場合の例を挙げる。OSPFについては、国際機関IETFで発行している仕様RFC2328、RFC1131、STD0054に詳細に記載されている。

【0028】OSPFで使用される経路形成情報、すなわちリンク状態広告パケット(LSA: Link State Advertisement)のうち、各ルータL11～L14が送信するルータリンクLSAのフォーマット例を図2に示す。このルータリンクLSAは、隣接ルータ間で受け渡される各種リンク情報であり、リンク状態ヘッダとLSA部とから構成される。LSA部には、ルータタイプ、リンクID、リンクデータ等が記述されており、これに記述される情報によって各ルータが他のルータの配置に関する情報を認識でき、経路計算、又は再計算に利用することができるようになる。図3は、ルータタイプの内容と、それに対するリンクID、リンクデータの例とを示したものである。タイプ1～4は、既存のルータが具備する情報であり、タイプ5が、本実施形態で追加した部分、つまり、暗号通信に関連する情報である。このタイプ5の記述によって、どのルータがどこで暗号通信を行っているかをわかるようにする。タイプ5において、リンクデータがNullの場合は、まだ決定されていないどこかと暗号通信ができることを示す。

【0029】LSAは、各ルータL11～L14で持てるリンク情報を複数発信することができる。従って、一つのルータが複数のルータとの間で暗号通信を行っていれば、暗号通信用LSAも複数指定できる。例えば、タイプ5のLSAでリンクIDが「163.135.100.10」、リンクデータが「163.135.20.0/24」であれば、このLSAを送信した「163.135.100.10」をアドレスとして持つルータは、「163.135.20.0/24」というアドレスを持つ

相手先と暗号通信ができる状態であることを示す。さらに、リンクIDまで同じで、リンクデータ「163.135.30.0/24」のLSAがあれば、ルータ「163.135.100.10」は、「163.135.30.0/24」の相手先とも暗号通信ができる状態であることを示す。

【0030】このような改良OSPFを使用し、パケットを暗号化して送信する場合、各ルータL11～L14は、暗号通信先の情報をLSAで宣言することになる。この宣言には、暗号通信元の情報も含まれる。各ルータL11～L14は、また、あるネットワークへ向かうパケットの復号化ができる場合、ルータ自身のデータベースにそのネットワークの情報を「暗号通信受け持ちネットワーク(又はホスト)」として記録する。この情報は、各ルータが、他のルータの暗号通信LSAを受け取ったときにその暗号通信先と同じ「暗号通信受け持ちネットワーク」を持っていた場合に、そのLSA送信元ルータとの間で鍵生成を行うために必要な情報となる。

【0031】ルータ同士は、それぞれHelloパケット(隣接ルータに対するキープアライブ信号のようなもの)の受け渡しを行っており、この受け渡しが可能なルータ間では、それぞれ自己のLSAがリンクバイーリンクで相手側に伝わるようになっている。例えば、BルータL13及びCルータL14が暗号化及び復号化が可能なルータである場合は、その旨及びそれが正常に動作していることが、DルータL12を通じてAルータL11に伝わる。AルータL11は、BルータL13のLSAにより、そのルータL13が自己の「暗号通信受け持ちネットワーク」と暗号通信を行う用意があることを知り、BルータL13との間で暗号用の鍵を生成するプロセスを実施する。このプロセスは、一般に用いられている鍵生成のプロセスであって構わない。AルータL11は、また、CルータL14の間でも鍵を生成するプロセスを実施する。

【0032】図4(a)は、通常経路で収束したときのAルータL11のリンクテーブル(ルーティングテーブルの元情報)の内容を示した図である。図示の例では、AルータL11は、αネットワーク及びDルータL12とリンクしており、暗号通信受け持ちネットワークはαとγである。BルータL13、CルータL14は、βネットワークとDルータL12とリンクしており、「暗号通信受け持ちネットワーク」は共にβである。Dルータは、AルータL11、BルータL13、CルータL14とリンクしており、「暗号通信受け持ちネットワーク」の指定がない又は未だ決定されていないどこかである。なお、「暗号通信受け持ちネットワーク」は、必ずしも隣接している必要はない。

【0033】このリンクテーブルから、AルータL11は、ネットワークαからネットワークβへの最適経路を、αネットワーク(通信装置T11)→AルータL11→DルータL12→BルータL13→βネットワーク

(通信装置 T12) のように形成する。

【0034】一方、A ルータ L11 は、図 4 (a) のリンクテーブルと連携して暗号化フィルタを図 5 (a) のように設定する。すなわち、A ルータ L11 の「暗号通信受け持ちネットワーク」は α ネットワークであり、経路上に β を「暗号通信受け持ちネットワーク」とするルータは B ルータ L13 である。そこで、A ルータ L11 は、B ルータ L13 との間で鍵 a の生成を行う (鍵 a を既に保持してある場合は、それを索出する)。このリンクテーブルの意味は、「発信元アドレス (ネットワーク) が α で、送信先アドレス (ネットワーク) が β のパケット ($\alpha \rightarrow \beta$) を、鍵 a で暗号化して B ルータ L13 へ送信 (set peer(B)) せよ」である。これにより鍵 a を用いた暗号通信が可能になる。

【0035】ここで、B ルータ L13 に障害が発生した場合を考える。この場合は、B ルータ L13 が発する LSA が D ルータ L12 及び A ルータ L11 に届かないため、A ルータ L11 は、ルーティングプロトコルの機能を用いて B ルータ L13 が使えないものとして経路を回復させる。図 4 (b) は、回復経路で収束したときの A ルータ L11 のリンクテーブル (ルーティングテーブルの元) の更新後の内容を示した図である。図示のように、B ルータ L13 のリンク情報が無くなっている。このリンクテーブルから、最適経路は、 α ネットワーク (通信装置 T11) \rightarrow A ルータ L11 \rightarrow D ルータ L12 \rightarrow C ルータ L14 \rightarrow β ネットワーク (通信装置 T12) のように変更されるが、本実施形態では更に、経路変更と連携して A ルータ L11 が使用する鍵 a を鍵 c に動的に変更させる。

【0036】すなわち、A ルータ L11 は、図 4 (b) のリンクテーブルが更新されると、これに連携して暗号化フィルタの内容を図 5 (b) のように更新する。すなわち、経路上に β を「暗号通信受け持ちネットワーク」とするルータは C ルータ L14 であることがわかるので、A ルータ L11 は、C ルータ L14 との間で鍵 c の生成を行う (鍵 c を既に保持してある場合は、それを索出する)。このリンクテーブルの意味は、「発信元アドレス (ネットワーク) が α で、送信先アドレス (ネットワーク) が β のパケット ($\alpha \rightarrow \beta$) を、鍵 c で暗号化して C ルータ L14 へ送信 (set peer(B)) せよ」である。

【0037】このように、B ルータ L13 に障害が発生し、経路変更がなされても、更新後のルーティングプロトコルによるリンクテーブルから図 5 (b) のような暗号化フィルタの設定が得られ、経路変更に伴う鍵の変更がなされるので、暗号通信を継続できるようになる。

【0038】なお、本実施形態では、暗号通信可能なルータの配置構成に変更が生じ、これによって使用する鍵が変更される場合の例として、ルータの故障等による経路障害が生じたことを想定したが、本発明は、このよう

な例のみではなく、例えばネットワーク上にルータを増設し、あるいはあるネットワークから他のネットワークにルータを移動させた結果、使用する鍵が変更される場合にも同様に適用が可能である。すなわち、手動による暗号通信の設定を行うことなく、ルーティングプロトコルの機能を用いて相互に経路形成情報を受け渡し、その配置情報を各ルータで更新し、最適経路を自動的に形成することで、暗号通信を継続することが可能である。また、ルータの経路形成情報に、暗号通信を行う対象のネットワークないしホストを指定するだけで、当該ルータが自動的に暗号通信を行う相手先装置を見つけ出すことも可能となる。これらの機能は、あるネットワーク上に接続されるルータの数が絶えず増減するという現実の通信形態に即した機能であり、これによってモバイル型通信の普及にも容易に対応が可能になるものである。

【0039】本実施形態では、通信中継装置としてルータを例に挙げて説明したが、本発明の仕組みは、暗号通信の相手先が変化する場合のある装置全般に適用することが可能である。また、本実施形態のように経路形成情報を他の装置と相互に受け渡し機能と暗号用の鍵を動的に変更させる機能とを一つの装置 (例えばルータ) 内に設けることは好ましい形態であるが、常にこのような形態にしなければならないというものではない。例えばルータに接続された通信装置が、ルータからの通知に基づいて暗号用の鍵を動的に変更する機能をもつように構成することは、本発明の暗号通信方法を実施する上で支障とはならない。

【0040】本実施形態では、IP ネットワークを通信媒体とした例について説明したが、本発明は、高可用通信と暗号通信とを同時に実現することができるネットワークであれば、その規模にかかわらず適用が可能なので、アンセキュアなネットワークであるイントラネットやエクストラネットでの利用も可能である。

【0041】本発明の適用には、ルーティングプロトコルのような経路形成情報の相互受け渡し機能が前提となるため、他の独自のルーティングプロトコルを使ったり、ルーティングプロトコルの相互接続ができない ISP (Internet Service Provider) を利用する場合は、その ISP を利用しない閉域網内で利用することになるが、その ISP を利用した場合であっても、経路形成情報を公知のトンネリング技術で ISP のサービスによらない方法で中継することにより、閉域網を越えたネットワークでの利用も可能である。

【0042】本発明は、暗号通信先が物理的もしくは論理的に頻繁に変更になる場合に特に有効であり、モバイルネットワークといった網構成変更にも柔軟に対応が可能である。

【0043】本発明は、また、コンシューマ用暗号通信市場 (個人を対象としたネットワークサービスの利用の一形態) への適用も可能である。現在、個人を対象とし

た暗号通信技術の主流はSSL (Secure Socket Layer) である。これは、通信の上位層で暗号化するもので、個人が操作する端末（通信装置）自らが通信データを暗号化して送信することによりエンド・ツー・エンドの暗号通信を行うことを目的とする。本発明をこの個人が操作する端末（モバイル型端末を含む）がアクセスするネットワークに適用させることは、上記ネットワークサービスを促進する上で有効な手段となり得る。

【0044】

【発明の効果】以上の説明から明らかなように、本発明によれば、暗号通信中に経路変更が行われた結果、復号化する装置、つまり鍵に変更が生じた場合であっても、暗号通信を安全且つ確実に継続できるようになるという、特有の効果がある。

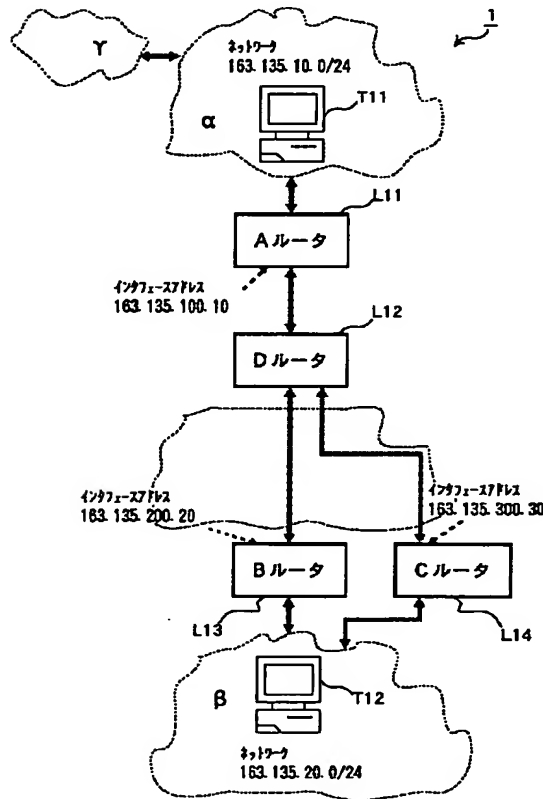
【図面の簡単な説明】

【図1】本発明を適用した暗号通信システムの構成図。

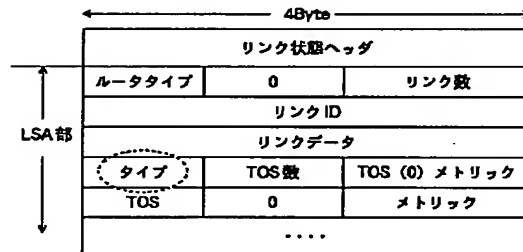
【図2】ルータリンクLSAのフォーマット例を示した図。

【図3】ルータリンクLSAのタイプ種類を示した図。＊

【図1】



【図2】



【図3】

タイプ	内容	リンクID	リンクデータ
1	他のネットワークへの接続	隣接ルータのルータID	インタフェース番号 (またはIPアドレス)
2	通過ネットワークへの接続	代表ルータへのアドレス	ルータのそのネットワーク上のIPアドレス
3	サブネットワークへの接続	サブネットワークアドレス、プレフィックス	プレフィックス長
4	仮想リンク	隣接ルータのルータID	ルータのそのネットワーク上のIPアドレス
5 (追加する部分)	暗号通信	暗号通信ができる自ノードのIPアドレスかルータID、またはインタフェース番号、またはインタフェースのIPアドレス	暗号通信ができる相手先のネットワークアドレスまたはホストアドレス

＊【図4】(a)は、ルーティングプロトコルを用いた場合の最適経路を形成する場合に使用されるリンクテーブルの内容説明図、(b)は障害発生時に更新されるリンクテーブルの内容説明図。

【図5】(a)は、正常動作時における暗号化フィルタの設定内容を示した図、(b)は障害発生時に更新される暗号化フィルタの設定内容を示した図。

【図6】従来における、ルーティングプロトコルを用いた場合の最適経路復旧の説明に用いるためのネットワーク構成図。

【図7】従来における、ルーティングプロトコル及び暗号通信を用いた場合の最適経路復旧の説明に用いるためのネットワーク構成図である。

【符号の説明】

1 暗号通信システム

T11, T12 通信装置

L11~L14, N11~N15 ルータ

M21~M23 暗号装置

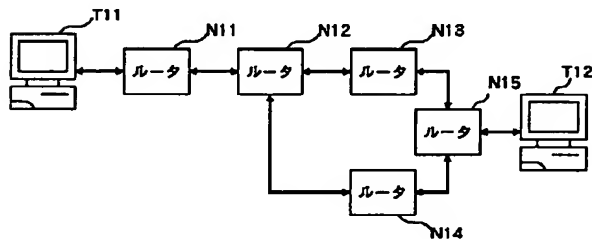
【図 4】

ルータ	A	B	C	D
持っているリンク (コスト)	α (1) D (1)	β (1) D (1)	β (1) D (2)	A (1) B (1) C (2)
暗号通信受け待ち ネットワーク	α γ	β	β	N/A

(b)

ルータ	A	C	D
持っているリンク (コスト)	α (1) D (1)	B (1) D (2)	A (1) B (1) C (2)
暗号通信受け待ち ネットワーク	α γ	β	N/A

【図 6】

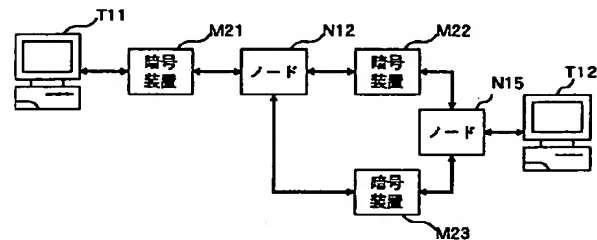


【図 5】

(a)	(b)
match	$\alpha \rightarrow \beta$
set peer	(B)
key	a

match	$\alpha \rightarrow \beta$
set peer	(C)
key	c

【図 7】



フロントページの続き

(51)Int.Cl.⁷
H 0 4 L 29/14

識別記号

F I

テーマコード (参考)

(72)発明者 馬場 達也
東京都江東区豊洲三丁目 3 番 3 号 株式会
社エヌ・ティ・ティ・データ内

F ターム (参考) 5J104 AA01 AA34 BA02 NA02 NA37
PA07
5K030 GA12 GA15 HD03 KA05 LB05
5K033 AA06 AA08 CB08 DA05 DB18
EC03
5K035 CC09 DD01 LL17
9A001 BB02 BB04 CC06 CC07 DD10
EE03 HH09 JJ18 LL07 LL09

Best Available Copy